PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2004-023597
(43)Date of publication of application : 22.01.2004

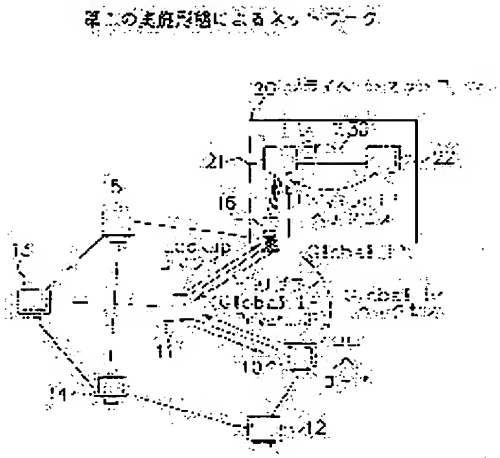
(51)Int.Cl. H04L 12/66
G06F 15/00

(21)Application number : 2002-178039
(22)Date of filing : 19.06.2002

(71)Applicant : ARIEL NETWORKS CO LTD
(72)Inventor : INOUE SEIICHIRO
HIDAKA TAKAHIRO
OTANI HIROYOSHI
IWATA SHINICHI

(54) NETWORK SYSTEM AND PROGRAM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a P2P (peer-to-peer) system that permits externally free access for acquisition of its resource even when the system is installed with a firewall or a NAT (network address translation) server.
SOLUTION: When a gateway node (NAT server) 16 for replacing a global address with a private address receives a hit reply from a node 21 in a private network 20, the node 16 attaches the information of the gateway node 16 to the information of a searching hit node 21 and propagates the added information. When a command issue source node 10 receiving the hit reply cannot establish an access session to the searching hit node 21, the node 10 selects the gateway node 16 in place of the node 21 and executes its access to the node 16 so that the node 10 can freely access the inside of the private network 20 from the outside to acquire a resource 30 even when the NAT server is present in the system.



LEGAL STATUS

[Date of request for examination] 25.05.2005
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-23597
(P2004-23597A)
(43)公開日　平成16年1月22日(2004.1.22)

(51)Int.Cl.[7]	F I		テーマコード（参考）
H04L 12/66	H04L 12/66	B	5B085
G06F 15/00	G06F 15/00	310D	5K030

審査請求 未請求　請求項の数 4　OL　（全 16 頁）

(21)出願番号　特願2002-178039(P2002-178039)
(22)出願日　平成14年6月19日(2002.6.19)

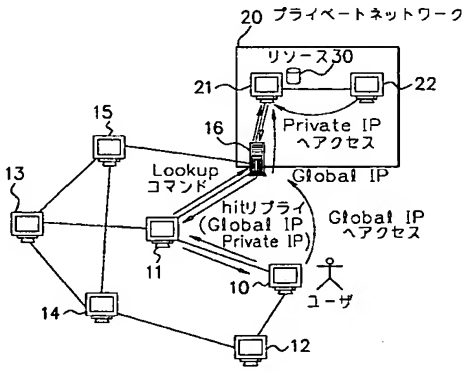
(71)出願人　502220160
アリエル・ネットワーク株式会社
東京都目黒区中目黒３－３－２　ＥＧビル７Ｆ
(74)代理人　100105784
弁理士　橘　和之
(72)発明者　井上　誠一郎
東京都世田谷区野毛２丁目１９番８号　グリーンハイムＡ１０３
(72)発明者　日高　孝寛
神奈川県川崎市高津区久本３丁目６番１２－２０８号
(72)発明者　大谷　弘喜
神奈川県平塚市袖が浜１７番４７－１０３号

最終頁に続く

(54)【発明の名称】ネットワークシステムおよびプログラム

(57)【要約】
【課題】ファイアフォールやＮＡＴサーバを設置した場合でも、外部から自由にアクセスしてリソースを取得可能なＰ２Ｐシステムを提供する。
【解決手段】グローバルアドレスとプライベートアドレスとの付け替えを行うゲートウェイノード（ＮＡＴサーバ）１６がプライベートネットワーク２０内のノード２１からｈｉｔリプライを受け取ったときに、検索ヒットノード２１の情報にゲートウェイノード１６の情報を加えて伝播するようにするとともに、ｈｉｔリプライを受け取ったコマンド発行元ノード１０から検索ヒットノード２１にアクセスのセッションが張れない場合に、ゲートウェイノード１６に切り替えてアクセスを実行するようにすることにより、ＮＡＴサーバが存在する場合でも、プライベートネットワーク２０の外部から内部へと自由にアクセスしてリソース３０を取得することができるようにする。
【選択図】　図１

第１の実施形態によるネットワーク



【特許請求の範囲】
【請求項１】
接続している近接ノード群にリソース検索コマンドを伝播していき、あるノードにおいてリソースの検索にヒットした場合、当該検索ヒットノードから検索ヒット応答を、上記リソース検索コマンドを伝播した各ノードにより逆向きに伝播してコマンド発行元ノードまで届けた後、上記コマンド発行元ノードが上記検索ヒットノードにアクセスして上記リソースを取得するように成されたネットワークシステムであって、
グローバルアドレスとプライベートアドレスとの付け替えを行うことによってプライベートネットワークの内外で通信のやり取りを行うゲートウェイノードを有し、当該ゲートウェイノードは、上記検索ヒット応答を受け取ったときに、上記検索ヒットノードの情報に上記ゲートウェイノードの情報を加えて上記検索ヒット応答を他のノードに転送する手段を備え、
各ノードは、自身が上記コマンド発行元ノードである場合に、上記検索ヒット応答中に含まれる上記検索ヒットノードの情報および上記ゲートウェイノードの情報に基づいて、上記検索ヒットノードもしくは上記ゲートウェイノードにアクセスする手段を備えたことを特徴とするネットワークシステム。
【請求項２】
接続している近接ノード群にリソース検索コマンドを伝播していき、あるノードにおいてリソースの検索にヒットした場合、当該検索ヒットノードから検索ヒット応答を、上記リソース検索コマンドを伝播した各ノードにより逆向きに伝播してコマンド発行元ノードまで届けた後、上記コマンド発行元ノードが上記検索ヒットノードにアクセスして上記リソースを取得するように成されたネットワークシステムであって、各ノードは、
自身が上記コマンド発行元ノードである場合において、上記検索ヒットノードにアクセスできないときに、上記接続している近接ノード群にアクセス要求コマンドを発行するアクセス要求手段と、
自身が上記検索ヒットノードである場合において、伝播されてきた上記アクセス要求コマンドを受け取ったときに、上記コマンド発行元ノードにアクセスを実行する逆アクセス手段とを備えたことを特徴とするネットワークシステム。
【請求項３】
上記各ノードは、自身が上記コマンド発行元ノードである場合において、上記アクセス要求コマンドを発行したにもかかわらず上記検索ヒットノードからのアクセスが確立されないときに、所定のゲートウェイノードにアクセスする第１のゲートウェイアクセス手段と、
上記ゲートウェイノードへのアクセスを要求するゲートウェイアクセス要求コマンドを上記接続している近接ノード群に発行する第２のアクセス要求手段と、自身が上記検索ヒットノードである場合において、伝播されてきた上記ゲートウェイアクセス要求コマンドを受け取ったときに、上記ゲートウェイノードにアクセスする第２のゲートウェイアクセス手段とを備えたことを特徴とする請求項２に記載のネットワークシステム。
【請求項４】
請求項１～３の何れか１項に記載の各手段としてコンピュータを機能させるためのプログラム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明はネットワークシステムおよびプログラムに関し、特に、サーバを介さずにクライアント同士で直接データの交換を行うシステムに用いて好適なものである。
【０００２】
【従来の技術】
近年、インターネットの浸透とインターネットユーザ数の爆発的増加という社会的背景、パーソナルコンピュータ（パソコン）の高性能化とネットワークの高速化という技術的背

景をもとに、ピアツーピア（Ｐ２Ｐ）と呼ばれるネットワーク技術が注目を集めている。

【０００３】

従来のネットワークシステムは、少数のサーバと多数のクライアントとをネットワークを介して接続したものが殆どであり、クライアントで生成されたリソースはサーバに集められて管理されていた。ところが、爆発的ユーザ数増加の中、ユーザの生み出したリソースをサーバに集めるコストは無視できないものになっている。

【０００４】

すなわち、従来のＷｅｂアーキテクチャにおいてサーバにリソースを集める際に、インターネット上に散らばっているリソースを発見するメカニズムには、ディレクトリサービスとサーチエンジンの２つのタイプが存在する。前者は人海戦術と呼ぶべきアプローチで、人手の作業によってリソースを集めるものである。後者はエージェントロボットがインターネットを巡回することによってリソースを集めてまわるものであり、何れのタイプも言わば力任せのアプローチである。

【０００５】

また、サーバに集められたリソースは、アクセスの集中を生む。この結果、クライアントとして用いられる高性能なパソコンは殆ど遊休状態となり、高速ネットワークもサーバ周辺だけがいびつに混雑する結果となっている。

【０００６】

これに対し、Ｐ２Ｐによるネットワーク技術は、ユーザに近い部分でサーバを介さずに、クライアント同士がダイレクトに情報のやり取りをするアーキテクチャである。つまり、多数のクライアントで生成されたリソースはそれぞれのクライアント自身で管理されるため、多数のリソースをサーバに集める必要もないし、リソース取得のためにアクセスの集中が生じることも殆どない。また、高性能なパソコンが持つ遊休資源を有効に使うことも可能となる。

【０００７】

図１１を参照して、Ｐ２Ｐアーキテクチャを利用して所望のリソースを検索および取得する際の手順を説明する。図１１は、Ｐ２Ｐアーキテクチャが適用されるネットワークの概略構成を示す図である。Ｐ２Ｐネットワークは、ノードの集合で定義される。ノードとは、Ｐ２Ｐプロトコルを実装したプログラムのプロセスのことを言う。したがって、例えば１つのパソコンの中にも、起動しているプログラムが複数あれば、複数のノードが存在することになる。

【０００８】

ノード同士は、複数のセッションを互いに張った状態でトポロジを形成する。この常態的なセッションを「接続」と呼ぶことにする。「接続」が常態的なトポロジ形成をなして、この接続セッション上を基本的なプロトコル（リソース検索コマンドに相当するｌｏｏｋｕｐコマンドや、検索ヒット応答に相当するｈｉｔリプライ等）が流れる。

【０００９】

これに対して、ユーザノード１００（ｌｏｏｋｕｐコマンドの発行元ノード）からリソース１１０の存在するノード１０３（ｈｉｔリプライの発行元ノード）に対して張るセッションを「アクセス」と呼ぶことにする。「アクセス」は、リソース発見後にコマンド発行元ノードと検索ヒットノードとの間に一時的に張られるセッションで、この上をアクセスインタフェースに応じたプロトコルが流れる。

【００１０】

上記した「接続」および「アクセス」のトポロジ形成の状態は中央で管理されず、個々のノードが自律的に形成する。まず、図１１（ａ）のように、リソース１１０の取得を希望しているユーザのノード１００は、どこにリソース１１０があるかを探し出すためのｌｏｏｋｕｐコマンドを近接ノード（接続しているノード）１０１，１０２に発行する。

【００１１】

ｌｏｏｋｕｐコマンド受け取ったノード１０１，１０２は、要求されているリソース１１０を自身が持っているかどうかを調べる。該当するリソース１１０が見つからない場合は

、図１１（ｂ）のように、ｌｏｏｋｕｐコマンドを近接ノード（ｌｏｏｋｕｐコマンドの送信元以外で接続しているノード）１０３～１０６に転送する。このｌｏｏｋｕｐコマンドを受け取ったノード１０３～１０６も、要求されているリソース１１０を自身が持っているかどうかを調べる。

【００１２】

このようにコマンド伝播とリソース１１０の検索を繰り返していく中で、ノード１０３では、リソース１１０の検索にヒットする。検索にヒットした場合は、図１１（ｃ）に示すように、ｌｏｏｋｕｐコマンドの送信元であるノード１０１にｈｉｔリプライを返す。ｈｉｔリプライを受け取ったノード１０１は、ｌｏｏｋｕｐコマンドの送信元であるユーザノード１００にｈｉｔリプライを転送する。このようにｈｉｔリプライは、ｌｏｏｋｕｐコマンドを伝播した各ノードにより逆向きに伝播され、コマンド発行元のユーザノード１００まで届けられる。

【００１３】

ｈｉｔリプライは、リソース１１０のアクセスインタフェースの名前と検索ヒットノード１０３の情報とを含むパケットである。以上の手順により、最初にｌｏｏｋｕｐコマンドを発行したユーザノード１００では、所望のリソース１１０がノード１０３に存在することを発見できる。ｈｉｔリプライを受け取ったユーザノード１００は次に、図１１（ｄ）のようにノード１０３にダイレクトにアクセスし、リソース１１０を取得する。

【００１４】

【発明が解決しようとする課題】

上述のようなＰ２Ｐアーキテクチャを利用して、種々のネットワークシステムを構築することが期待されている。例えば、Ｐ２Ｐプロトコルをベースにして、個人またはグループのスケジュールやタスクの管理、文書等のファイル管理、プロジェクトの進捗管理などを行うグループウェアなどを構築することが望まれている。

【００１５】

しかしながら、上記従来のＰ２Ｐネットワーク技術では、ファイアウォールやＮＡＴ（Ｎｅｔｗｏｒｋ　Ａｄｄｒｅｓｓ　Ｔｒａｎｓｌａｔｉｏｎ）があると、グループ内向きのセッションが張れず（接続やアクセスができない）、通信上の大きな障害が発生するという問題があった。

【００１６】

ファイアウォールは、一般的には１台のサーバをグループの出入口に用い、ここで専用のソフトウェアを動作させることによって、アクセス権を持たない第三者がグループ内に不正に侵入するのを防ぐものである。具体的には、送信元と送信先のＩＰアドレスを見て通信の可否を判断する。したがって、ファイアフォールが設置されていると、グループの外側から内側に向けての通信が拒否され、接続およびアクセスのセッションを張ることができなくなってしまう。

【００１７】

また、ＮＡＴは、ＩＰアドレスの不足に対応するために考え出された手法である。これは、グループの出入口となるゲートウェイにだけグローバルアドレスを割り振り、グループ内部では当該グループ内でのみ通用するプライベートアドレスを割り振ることにより、グローバルアドレスを節約しようとするものである。ゲートウェイとなるＮＡＴサーバは、グループ外部から送られてきたグローバルアドレスをプライベートアドレスに変換することにより、グループ内のノードにアクセスする。

【００１８】

したがって、ゲートウェイとしてＮＡＴサーバが設置されている場合、ｌｏｏｋｕｐコマンドの発行元ノードがグループの外側にあり、コマンド伝播によって発見されたノードがグループの内側にあると、グローバルアドレスを持つ外部ノードからプライベートアドレスを持つ内部ノードに対して直接アクセスのセッションを張ることができなくなってしまう。

【００１９】

Ｐ２Ｐアーキテクチャを用いてグループウェアを構築する場合、グループ内のデータが第三者によって不正に盗聴または改ざんされる危険性から守るのと同時に、グループのメンバが外部からもアクセスできるようにすることが望まれる。ＬＡＮが構築されている社内だけでなく、自宅や外出先からアクセスできるようにすることが好ましいからである。しかし、セキュリティ対策やＩＰアドレス確保のためにファイアフォールやＮＡＴサーバを設置すると、上述のように内向きのセッションが張れなくなり、外部からのアクセスができないという問題があった。

【００２０】

本発明は、このような問題を解決するために成されたものであり、ファイアフォールやＮＡＴサーバを設置した場合でも、外部から自由にアクセスしてリソースを取得可能なＰ２ＰシステムＰを提供することを目的とする。

【００２１】

【課題を解決するための手段】

本発明のネットワークシステムは、グローバルアドレスとプライベートアドレスとの付け替えを行うことによってプライベートネットワークの内外で通信のやり取りを行うゲートウェイノードを有し、当該ゲートウェイノードは、検索ヒット応答を受け取ったときに、検索ヒットノードの情報にゲートウェイノードの情報を加えて検索ヒット応答を他のノードに転送する手段を備え、各ノードは、自身がコマンド発行元ノードである場合に、検索ヒット応答中に含まれる検索ヒットノードの情報およびゲートウェイノードの情報に基づいて、検索ヒットノードもしくはゲートウェイノードにアクセスする手段を備えたことを特徴とする。

【００２２】

本発明の他の態様では、各ノードが、自身がコマンド発行元ノードである場合において、検索ヒットノードにアクセスできないときに、接続している近接ノード群にアクセス要求コマンドを発行するアクセス要求手段と、自身が検索ヒットノードである場合において、伝播されてきたアクセス要求コマンドを受け取ったときに、コマンド発行元ノードにアクセスを実行する逆アクセス手段とを備えたことを特徴とする。

【００２３】

本発明の他の態様では、各ノードが、自身がコマンド発行元ノードである場合において、アクセス要求コマンドを発行したにもかかわらず検索ヒットノードからのアクセスが確立されないときに、所定のゲートウェイノードにアクセスする第１のゲートウェイアクセス手段と、ゲートウェイノードへのアクセスを要求するゲートウェイアクセス要求コマンドを、接続している近接ノード群に発行する第２のアクセス要求手段と、自身が検索ヒットノードである場合において、伝播されてきたゲートウェイアクセス要求コマンドを受け取ったときに、ゲートウェイノードにアクセスする第２のゲートウェイアクセス手段とを備えたことを特徴とする。

【００２４】

【発明の実施の形態】

（第１の実施形態）

以下、本発明の第１の実施形態を図面に基づいて説明する。

図１は、第１の実施形態によるネットワークの概略構成例を示す図である。本実施形態のネットワークは、ノードの集合１０～１６，２１～２２を含んで構成されている。

【００２５】

図１の例において、ノード２１，２２によってプライベートネットワーク２０が構成されている。したがって、このノード２１，２２間では、プライベートＩＰアドレス（以下、プライベートＩＰと略す）に基づいてアクセスが行われる。一方、ノード１０～１６は、プライベートネットワーク２０の外部に存在するノードである。したがって、これらのノード１０～１６間では、グローバルＩＰアドレス（以下、グローバルＩＰと略す）に基づいてアクセスが行われる。

【００２６】

ノード１６はＮＡＴサーバであり、グローバルＩＰとプライベートＩＰとの双方を持つ。プライベートネットワーク２０の外部からパケットが送られてきたときは、その宛て先グローバルＩＰ（ＮＡＴサーバ１６のグローバルＩＰ）をプライベートＩＰに変換することにより、プライベートネットワーク２０内のノード２１にアクセスする。逆に、プライベートネットワーク２０内のノード２１からパケットが送られてきたときは、その送信元プライベートＩＰ（ノード２１のプライベートＩＰ）をＮＡＴサーバ１６のグローバルＩＰに変換して外部のノードにアクセスする。

【００２７】

本実施形態では、ＮＡＴサーバ１６のポートフォワード機能を利用して、Ｐ２Ｐアーキテクチャ用のポートを転送する設定を行う。すなわち、マスカレードノードとしてＮＡＴサーバ１６を設定する。これによりＮＡＴサーバ１６は、ｈｉｔリプライを転送するときに、リソースの検索にヒットした検索ヒットノードの情報と、マスカレードノードであるＮＡＴサーバ１６の情報との双方を転送するように処理する。

【００２８】

例えば、図１のようにｌｏｏｋｕｐコマンドの発行元ノード１０がプライベートネットワーク２０の外部にあり、所望のリソース３０を備えた検索ヒットノード２１がプライベートネットワーク２０の内部にある場合について考える。この場合においてＮＡＴサーバ１６は、検索ヒットノード２１から送られてきたｈｉｔリプライを転送するときに、検索ヒットノード２１のプライベートＩＰに対して、マスカレードノードであるＮＡＴサーバ１６のグローバルＩＰを加えて、その両方のノード情報を転送するようにする。

【００２９】

このｈｉｔリプライを受信したコマンド発行元ノード１０は、ｈｉｔリプライ中に含まれている検索ヒットノード２１のプライベートＩＰに基づいて、通常の処理に従って当該検索ヒットノード２１にアクセスを試みる。

【００３０】

しかし、コマンド発行元ノード１０から検索ヒットノード２１に対してはアクセスのセッションを直接張ることができない。そこで、コマンド発行元ノード１０は、ｈｉｔリプライ中に含まれているＮＡＴサーバ１６のグローバルＩＰに基づいて、マスカレードノードへのアクセスに切り替えて検索ヒットノード２１に間接的にアクセスする。

【００３１】

図２は、ＮＡＴサーバ１６の動作を示すフローチャートである。このフローチャートは、ＮＡＴサーバ１６が他のノードから何らかのコマンドを受信した際の動作を示すものである。図２において、ＮＡＴサーバ１６は、受信したコマンドがｌｏｏｋｕｐコマンドかどうかを判断し（ステップＳ１）、そうであればそのｌｏｏｋｕｐコマンドを他のノードに伝播する（ステップＳ２）。

【００３２】

受信したコマンドがｌｏｏｋｕｐコマンドでない場合は、更にｈｉｔリプライであるかどうかを判断する（ステップＳ３）。ｈｉｔリプライでもない場合は、その受信したコマンドに従ってその他の処理を行う（ステップＳ４）。一方、ｈｉｔリプライを受信した場合、ＮＡＴサーバ１６は、マスカレードノードとして動作する自身のグローバルＩＰをｈｉｔリプライ中に付加し（ステップＳ５）、当該グローバルＩＰの付加されたｈｉｔリプライを他のノードに伝播する（ステップＳ６）。

【００３３】

また、図３は、コマンド発行元ノード１０の動作を示すフローチャートである。このフローチャートは、コマンド発行元ノード１０が他のノードからｈｉｔリプライを受信した際の動作を示すものである。図３において、コマンド発行元ノード１０は、受信したｈｉｔリプライ中に含まれている検索ヒットノード２１のプライベートＩＰに基づいて、当該検索ヒットノード２１にアクセスを試みる（ステップＳ１１）。

【００３４】

そして、アクセスのセッションが張れたかどうかを判断する（ステップＳ１２）。プライ

ベートネットワーク２０の内部同士あるいは外部同士でアクセスするような場合には、セッションを張ることができる。したがって、例えば検索ヒットノードもコマンド発行元ノード１０と同様にプライベートネットワーク２０の外部にあるような場合には、コマンド発行元ノード１０はそのアクセスに基づいて検索ヒットノードからリソースを取得する（ステップＳ１４）。

【００３５】

ただし、今の例では、検索ヒットノード２１がプライベートネットワーク２０の内部にあるので、プライベートネットワーク２０の外部にあるコマンド発行元ノード１０からその検索ヒットノード２１に対してはアクセスのセッションを張ることができない。この場合、コマンド発行元ノード１０は、ｈｉｔリプライ中に含まれているＮＡＴサーバ１６のグローバルＩＰに基づいて、マスカレードノードへのアクセスに切り替えて検索ヒットノード２１にアクセスし（ステップＳ１３）、リソースを取得する（ステップＳ１４）。

【００３６】

以上詳しく説明したように、第１の実施形態によれば、ｈｉｔリプライにマスカレードノードとしてのＮＡＴサーバのグローバルＩＰを付加して伝播するとともに、コマンド発行元ノードが検索ヒットノードにアクセスしてセッションを張れないときはマスカレードノードへのアクセスに切り替えて検索ヒットノードにアクセスするようにしたので、ＮＡＴサーバが設置されている場合でも、プライベートネットワークの外部から内部へと自由にアクセスすることができるようになる。

【００３７】

（第２の実施形態）

次に、本発明の第２の実施形態を図面に基づいて説明する。

図４は、第２の実施形態によるネットワークの概略構成例を示す図である。本実施形態のネットワークは、ノードの集合１０～１５，２１を含んで構成されている。

【００３８】

図４の例において、ノード２１はファイアウォール４０の内部にあるものとする。また、その他のノード１０～１５はファイアウォール４０の外部にあるものとする。本実施形態において、接続のセッションは、張れない場合には対処しない。しかし、接続セッションをファイアウォール４０の内部または外部のどちらから張るかは問題でなく、張れる方向のみで接続セッションを開始して、トポロジを形成する。

【００３９】

図４の例では、ファイアウォール４０内のノード２１から外部のノード１１，１５に対してセッションを開始することにより、これらの間に既に接続が確立している状態を示している。このような状態で、ノード１０からリソース３０を検索するためのｌｏｏｋｕｐコマンドを発行した結果、ノード１１を経由してファイアウォール４０内のノード２１にｌｏｏｋｕｐコマンドが伝播され、当該ノード２１から逆の流れでｈｉｔリプライが返されてきたとする。

【００４０】

ｈｉｔリプライを受け取ったコマンド発行元ノード１０は、通常の処理に従って、検索ヒットノード２１に対してダイレクトにアクセスを試みる。しかし、検索ヒットノード２１はファイアウォール４０の内部に存在するので、コマンド発行元ノード１０から検索ヒットノード２１に対してはアクセスのセッションを張ることができない。

【００４１】

この場合、コマンド発行元ノード１０は、接続のセッションを通して、検索ヒットノード２１に対してｐｕｓｈ－ｒｅｑコマンド（アクセス要求コマンド）を発行する。このｐｕｓｈ－ｒｅｑコマンドは、ｈｉｔリプライが逆伝播された経路に従って、検索ヒットノード２１に届けられる。ｐｕｓｈ－ｒｅｑコマンドは、コマンド発行元ノード１０の情報を含むパケットである。したがって、このｐｕｓｈ－ｒｅｑコマンドを受信した検索ヒットノード２１では、コマンド発行元ノード１０を知ることができる。

【００４２】

そこで、ｐｕｓｈ－ｒｅｑコマンドを受け取った検索ヒットノード２１は、コマンド発行元ノード１０に対してアクセスする。これは、通常のアクセス時と逆向きのセッションの張り方となる。ここでは、ファイアウォール４０の内側から外側に向かうアクセスなので、問題なくセッションを張ることができる。コマンド発行元ノード１０は、このとき張られたアクセスのセッションを通じて検索ヒットノード２１にアクセスし、リソース３０を取得する。

【００４３】

図５は、図４に示したコマンド発行元ノード１０の動作を示すフローチャートである。このフローチャートは、コマンド発行元ノード１０が他のノードからｈｉｔリプライを受信した際の動作を示すものである。図５において、コマンド発行元ノード１０は、受信したｈｉｔリプライ中に含まれているアクセスインタフェースの名前および検索ヒットノード２１の情報に基づいて、検索ヒットノード２１にアクセスを試みる（ステップＳ２１）。

【００４４】

そして、アクセスのセッションが張れたかどうかを判断する（ステップＳ２２）。ファイアウォール４０の外部同士あるいはファイアウォール４０の内部から外部へのアクセスをするような場合には、セッションを張ることができる。その場合、コマンド発行元ノード１０はそのアクセスに基づいて検索ヒットノードからリソースを取得する（ステップＳ２６）。

【００４５】

ただし、図４のようにファイアウォール４０の外部から内部の検索ヒットノード２１にアクセスするような場合は、アクセスのセッションを張ることができない。この場合、コマンド発行元ノード１０は、ｐｕｓｈ－ｒｅｑコマンドを発行する（ステップＳ２３）。その後、そのｐｕｓｈ－ｒｅｑコマンドに従って検索ヒットノード２１からアクセスが行われたかどうかを判断し（ステップＳ２４）、行われた場合には、そのアクセスのセッションを通じて検索ヒットノード２１にアクセスして（ステップＳ２５）、リソース３０を取得する（ステップＳ２６）。

【００４６】

図６は、第２の実施形態によるネットワークの別の構成例を示す図である。図６に示す例では、検索ヒットノード２１がファイアウォール４０の内部にあるだけでなく、コマンド発行元ノード１０も別のファイアウォール４１の内部に含まれている。このような場合に対応するために、アクセスの仲介を行うためのゲートウェイノード（ＧＷノード）５０を各ファイアウォール４０，４１の外部に用意する。ゲートウェイノード５０は、コマンド発行元ノード１０および検索ヒットノード２１の両方からセッションを張れる必要がある。

【００４７】

この図６の例においても、ノード１０からリソース３０を検索するためのｌｏｏｋｕｐコマンドを発行した結果、ノード１１を経由してファイアウォール４０内のノード２１にｌｏｏｋｕｐコマンドが伝播され、当該ノード２１から逆の流れでｈｉｔリプライが返されてきたとする。

【００４８】

ｈｉｔリプライを受け取ったコマンド発行元ノード１０は、通常の処理に従って、検索ヒットノード２１に対してダイレクトにアクセスを試みる。しかし、検索ヒットノード２１はファイアウォール４０の内部に存在するので、コマンド発行元ノード１０から検索ヒットノード２１に対してはアクセスのセッションを張ることができない。

【００４９】

この場合、コマンド発行元ノード１０は、ｈｉｔリプライが逆伝播された接続経路に沿って、検索ヒットノード２１に対してｐｕｓｈ－ｒｅｑコマンドを発行する。ｐｕｓｈ－ｒｅｑコマンドを受け取った検索ヒットノード２１は、コマンド発行元ノード１０に対してアクセスを試みる。これは、通常のアクセス時と逆向きのセッションの張り方となる。

【００５０】

先に示した図４の例では、この時点でアクセスのセッションを張ることができた。しかし、ここでは、コマンド発行元ノード１０もファイアウォール４１の内部に存在するので、検索ヒットノード２１からコマンド発行元ノード１０に対してもアクセスのセッションを張ることができない。

【００５１】

この場合、コマンド発行元ノード１０は、接続のセッションを通して、検索ヒットノード２１に対してｇｗ－ｒｅｑコマンド（ゲートウェイアクセス要求コマンド）を発行する。このｇｗ－ｒｅｑコマンドは、ｈｉｔリプライが逆伝播された経路に従って、検索ヒットノード２１に届けられる。ｇｗ－ｒｅｑコマンドは、ゲートウェイノード５０の情報を含むパケットである。したがって、このｇｗ－ｒｅｑコマンドを発行したコマンド発行元ノード１０およびこれを受信した検索ヒットノード２１の双方は、ゲートウェイノード５０を知ることができる。

【００５２】

そこで、コマンド発行元ノード１０および検索ヒットノード２１は、ゲートウェイノード５０に対してアクセスする。これらは共に、ファイアウォール４０の内側から外側に向かうアクセスなので、問題なくセッションを張ることができる。ゲートウェイノード５０は、内部的に２つのセッションを結び付けて、アクセスのセッションを仲介する。コマンド発行元ノード１０は、このとき張られたアクセスセッションを通じて検索ヒットノード２１にアクセスし、リソース３０を取得する。

【００５３】

図７は、図６に示したコマンド発行元ノード１０の動作を示すフローチャートである。このフローチャートは、コマンド発行元ノード１０が他のノードからｈｉｔリプライを受信した際の動作を示すものである。図７において、コマンド発行元ノード１０は、受信したｈｉｔリプライ中に含まれているアクセスインタフェースの名前および検索ヒットノード２１の情報をもとに、検索ヒットノード２１にアクセスを試みる（ステップＳ３１）。

【００５４】

そして、アクセスのセッションが張れたかどうかを判断する（ステップＳ３２）。ここでアクセスのセッションを張ることができた場合、コマンド発行元ノード１０はそのアクセスに基づいて検索ヒットノードからリソースを取得する（ステップＳ３８）。

【００５５】

一方、図６のようにファイアウォール４０の外部から内部の検索ヒットノード２１にアクセスするような場合は、アクセスのセッションを張ることができない。この場合、コマンド発行元ノード１０は、ｐｕｓｈ－ｒｅｑコマンドを発行する（ステップＳ３３）。その後、そのｐｕｓｈ－ｒｅｑコマンドに従って検索ヒットノード２１からアクセスが行われたかどうかを判断し（ステップＳ３４）、行われた場合には、そのアクセスのセッションを通じて検索ヒットノード２１にアクセスして（ステップＳ３５）、リソース３０を取得する（ステップＳ３８）。

【００５６】

しかし、図６の例では検索ヒットノード２１からコマンド発行元ノード１０に対してもアクセスのセッションを張ることができない。この場合、コマンド発行元ノード１０は、検索ヒットノード２１に対してｇｗ－ｒｅｑコマンドを発行した後（ステップＳ３６）、ゲートウェイノード５０にアクセスする（ステップＳ３７）。検索ヒットノード２１にｇｗ－ｒｅｑコマンドを発行することによって、検索ヒットノード２１からもゲートウェイノード５０へのアクセスが行われるので、コマンド発行元ノード１０はこれらのアクセスセッションを通じて検索ヒットノード２１にアクセスし、リソース３０を取得する（ステップＳ３８）。

【００５７】

図８は、図６に示した検索ヒットノード２１の動作を示すフローチャートである。このフローチャートは、検索ヒットノード２１が他のノードにｈｉｔリプライを発行した後の動作を示すものである。図８において、検索ヒットノード２１は、ｐｕｓｈ－ｒｅｑコマン

ドを受信したかどうかを判断する（ステップＳ４１）。ｐｕｓｈ－ｒｅｑコマンドを受信していない場合は、コマンド発行元ノード１０から検索ヒットノード２１に対するアクセスのセッションがうまく張られたということなので、何もせずに処理を終了する。

【００５８】

一方、ｐｕｓｈ－ｒｅｑコマンドを受信した場合は、その受信したｐｕｓｈ－ｒｅｑコマンド中に含まれているコマンド発行元ノード１０の情報をもとに、当該コマンド発行元ノード１０にアクセスを試みる（ステップＳ４２）。そして、アクセスのセッションが張れたかどうかを判断する（ステップＳ４３）。ここでアクセスのセッションを張ることができた場合は、何もせずに処理を終了する。

【００５９】

検索ヒットノード２１からコマンド発行元ノード１０に対してアクセスのセッションを張ることができなかった場合、検索ヒットノード２１はｇｗ－ｒｅｑコマンドの受信待ちの状態になる（ステップＳ４４）。ｇｗ－ｒｅｑコマンドを受信した場合は、その受信したｇｗ－ｒｅｑコマンド中に含まれているゲートウェイノード５０の情報をもとに、当該ゲートウェイノード５０にアクセスして（ステップＳ４５）処理を終了する。

【００６０】

以上詳しく説明したように、第２の実施形態によれば、ファイアウォール内のリソースに外部からアクセスしようとする場合に、所定のコマンドを発行することによってファイアウォールの内側から外側に向かってアクセスのセッションを張るようにしたので、セキュリティ対策のためにファイアフォールを設置した場合でも、そのファイアウォールの外部から内部のリソースへと自由にアクセスすることができるようになる。

【００６１】

なお、このようにファイアウォールの内向きに自由にアクセスできるようになると、不正な第三者がグループのメンバに成りすましてファイアウォール内に侵入することもあり得る。本実施形態では、このような場合にも機密情報が漏れないように、転送するデータやファイル等のリソースを暗号化する。また、ユーザ認証も利用する。なお、暗号化の方式は特に限定しないが、例えばＰＫＩ（公開鍵暗号方式）を利用することが可能である。

【００６２】

本実施形態では、ユーザログイン時に認証のタイプを指定することができるようにしている。認証には、単純なパスワード認証から複雑なＳＳＬ（Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔｓ　Ｌａｙｅｒ）認証まで用意されている。パスワード認証は、各ノード上で実行される。ＳＳＬ認証は、各ノードが接続時に提出する証明書をベースにして行われる。

【００６３】

図９は、ユーザ情報を告知する際の動作を説明するための図である。図９に示すように、ユーザノード１０は、ネットワークへのログイン後および新たな接続の開始時に、接続セッションを利用してユーザ情報を告知する。このユーザ情報は、ユーザＩＤ、表示名、説明、ユーザ認証の証明書（公開鍵）を含む。ユーザノード１０から告知されたユーザ情報のパケットは、他のノード１１～１９間で伝播される。

【００６４】

ユーザノード１０から伝播されたユーザ情報は、各ノード１１～１９のローカルストレージが備える共通ユーザリスト６１，６２，・・・に各々キャッシュ記憶される。ユーザ認証やデータの暗号化あるいは復号化を行うときは、この共通ユーザリスト６１，６２，・・・に記憶されたユーザ情報を取得して利用する。

【００６５】

図１０は、ＳＳＬベースのユーザ認証を行う際の動作を説明するための図である。ＳＳＬ認証を行う場合、認証する側には、認証局の証明書が必要となる。そのためノードは、所定の属性ファイルと認証局の証明書とをセットで配布する。図９で説明したように、ノードにユーザがログインすると、ユーザノード１０は、その接続先にユーザの証明書を提出する。ユーザの証明書を受けたノードは、認証局の証明書で当該ユーザ証明書を認証する。証明書の認証後、ユーザの秘密鍵の本人確認を行い、これに認められた場合にログイン

を許可する。

【００６６】

ユーザ認証時に提出された証明書は、ユーザ情報の告知として他のノードに伝播される。各ノードは、受け取ったユーザ証明書をローカルストレージにキャッシュする。リソースをＳＳＬベースで暗号化するときや、リソースの署名を確認するときなどは、ユーザ証明書内の公開鍵を使用する。

【００６７】

このように、本実施形態では、ネットワークへのログイン時などにユーザ情報の告知を行うようにし、そのユーザ情報の中にユーザ証明書（公開鍵を含む）を含ませるようにしたので、各ノードに対して公開鍵を容易に配布することができる。逆に言えば、各ノードで公開鍵を入手するのが非常に容易であり、Ｐ２Ｐネットワークの中でユーザ認証および暗号化を容易に行うことができる。

【００６８】

以上に説明した本実施形態によるネットワークシステムの機能は、実際にはコンピュータのＣＰＵあるいはＭＰＵ、ＲＡＭ、ＲＯＭなどで構成され、ＲＡＭやＲＯＭに記憶されたプログラムが動作することによって実現できる。したがって、コンピュータが上記の機能を果たすように動作させるプログラムを例えばＣＤ－ＲＯＭのような記録媒体に記録し、コンピュータに読み込ませることによって実現できるものである。

【００６９】

上記プログラムを記録する記録媒体としては、ＣＤ－ＲＯＭ以外に、フレキシブルディスク、ハードディスク、磁気テープ、光ディスク、光磁気ディスク、ＤＶＤ、不揮発性メモリカード等を用いることができる。また、上記プログラムをインターネット等のネットワークを介してコンピュータにダウンロードすることによっても実現できる。

【００７０】

また、コンピュータが供給されたプログラムを実行することにより上述の実施形態の機能が実現されるだけでなく、そのプログラムがコンピュータにおいて稼働しているＯＳ（オペレーティングシステム）あるいは他のアプリケーションソフト等と共同して上述の実施形態の機能が実現される場合や、供給されたプログラムの処理の全てあるいは一部がコンピュータの機能拡張ボードや機能拡張ユニットにより行われて上述の実施形態の機能が実現される場合も、かかるプログラムは本実施形態に含まれる。

【００７１】

なお、上記に説明した各実施形態は、本発明を実施するにあたっての具体化の一例を示したものに過ぎず、これらによって本発明の技術的範囲が限定的に解釈されてはならないものである。すなわち、本発明はその精神、またはその主要な特徴から逸脱することなく、様々な形で実施することができる。

【００７２】

【発明の効果】

本発明は上述したように、グローバルアドレスとプライベートアドレスとの付け替えを行うゲートウェイノードが検索ヒット応答を受け取ったときに、検索ヒットノードの情報にゲートウェイノードの情報を加えて伝播するようにし、コマンド発行元ノードが検索ヒット応答を受け取ったときは、当該検索ヒット応答中に含まれる検索ヒットノードの情報およびゲートウェイノードの情報に基づき検索ヒットノードもしくはゲートウェイノードにアクセスするようにしている。これにより、ゲートウェイノードが存在する場合でも、プライベートネットワークの外部から内部あるいはその逆へと自由にアクセスしてリソースを取得することができるようになる。

【００７３】

本発明の他の特徴によれば、コマンド発行元ノードが検索ヒットノードにアクセスできないときに、接続している近接ノード群を介してアクセス要求コマンドを検索ヒットノードに伝播するとともに、これを受け取った検索ヒットノードがコマンド発行元ノードにアクセスを実行するようにしている。これにより、ファイアウォールの外側から内側に向かっ

てアクセスできない場合でも、上記アクセス要求コマンドを発行することによってファイアウォールの内側から外側に向かってアクセスを確立することができ、そのセッションを利用してファイアウォールの外部から内部のリソースへと自由にアクセスすることができるようになる。

【００７４】

また、本発明の他の特徴によれば、コマンド発行元ノードがアクセス要求コマンドを発行したにもかかわらず検索ヒットノードからのアクセスが確立されないときに、所定のゲートウェイノードにアクセスするとともに、当該ゲートウェイノードへのアクセス要求コマンドを近接ノード群を介して検索ヒットノードに伝播し、これを受け取った検索ヒットノードがゲートウェイノードにアクセスを実行するようにしている。これにより、コマンド発行元ノードと検索ヒットノードとの双方がファイアウォールの中にある場合であっても、それぞれのファイアウォールの内側から外側のゲートウェイノードに向かってアクセスを確立することができ、それらのセッションを利用してファイアウォールの外部から内部のリソースへと自由にアクセスすることができるようになる。

【図面の簡単な説明】

【図１】第１の実施形態によるネットワークの概略構成例を示す図である。

【図２】第１の実施形態によるＮＡＴサーバの動作を示すフローチャートである。

【図３】第１の実施形態によるコマンド発行元ノードの動作を示すフローチャートである。

【図４】第２の実施形態によるネットワークの概略構成例を示す図である。

【図５】図４に示したコマンド発行元ノードの動作を示すフローチャートである。

【図６】第２の実施形態によるネットワークの別の構成例を示す図である。

【図７】図６に示したコマンド発行元ノードの動作を示すフローチャートである。

【図８】図６に示した検索ヒットノードの動作を示すフローチャートである。

【図９】ユーザ情報の告知動作を示すフローチャートである。

【図１０】ＳＳＬベースのユーザ認証を行う際の動作を説明するための図である。

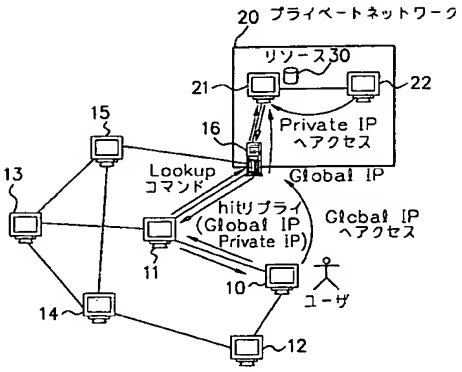
【図１１】Ｐ２Ｐアーキテクチャを利用して所望のリソースを検索および取得する際の手順を示す図である。

【符号の説明】

１０～１５　ノード
１６　マスカレードノード（ＮＡＴサーバ）
２０　プライベートネットワーク
２１～２２　ノード
３０　リソース
４０，４１　ファイアウォール
５０　ゲートウェイノード
６１，６２　共通ユーザリスト

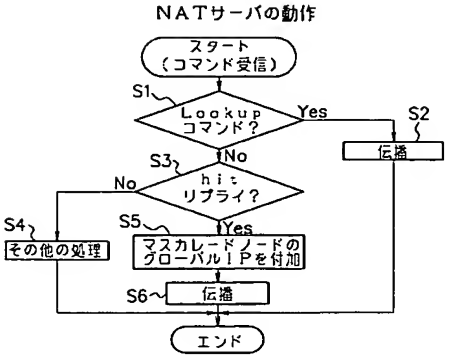
【図１】

第１の実施形態によるネットワーク



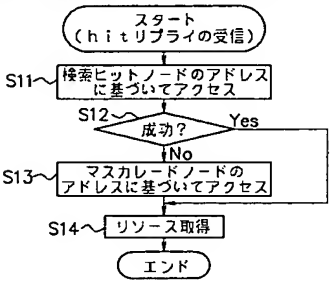
【図２】

NATサーバの動作



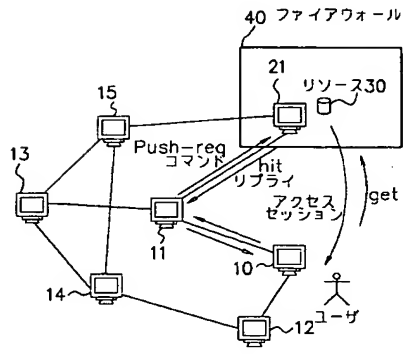
【図３】

第１の実施形態によるコマンド発行元ノードの動作



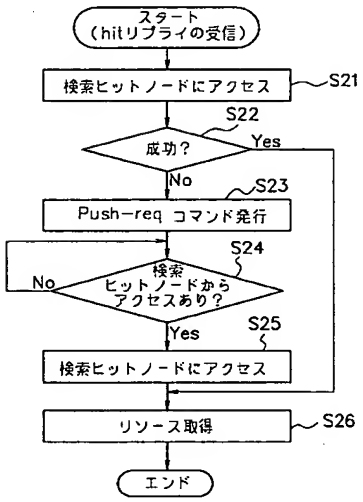
【図４】

第２の実施形態によるネットワーク



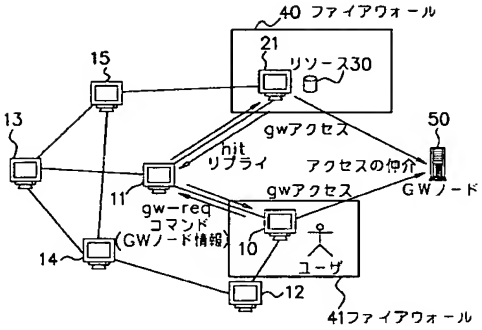
【図５】

第２の実施形態によるコマンド発行元ノードの動作



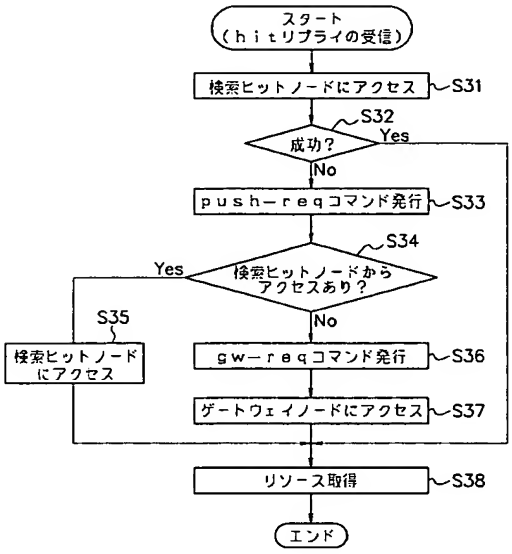
【図６】

第２の実施形態によるネットワークの別の例



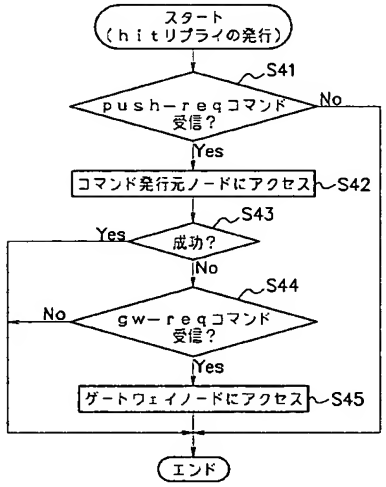
【図７】

第２の実施形態によるコマンド発行元ノードの他の動作



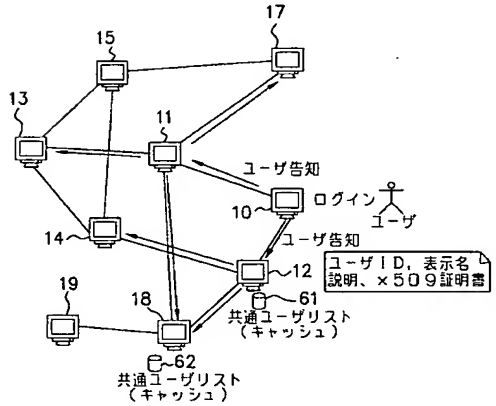
【図８】

第２の実施形態による検索ヒットノードの動作

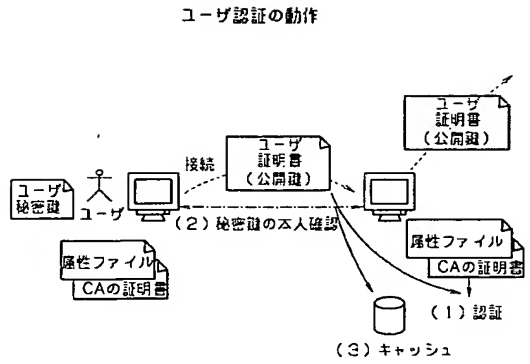


【図９】

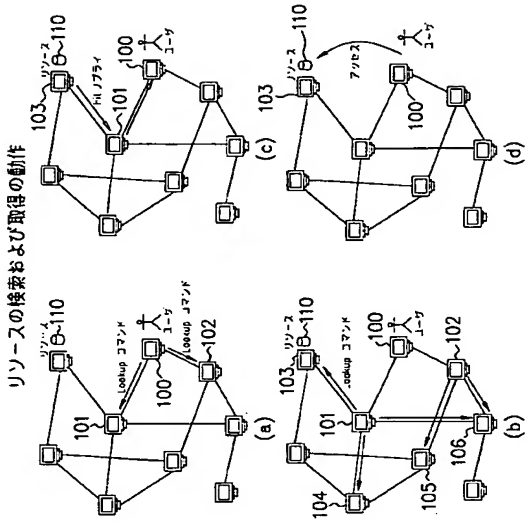
ユーザ情報の告知動作



【図１０】


ユーザ認証の動作
ユーザ秘密鍵
ユーザ
接続
ユーザ証明書（公開鍵）
ユーザ証明書（公開鍵）
（２）秘密鍵の本人確認
属性ファイル
CAの証明書
属性ファイル
CAの証明書
（１）認証
（３）キャッシュ

【図１１】


リソースの検索および取得の動作
リソースB
ユーザ
100
101
102
103
104
105
106
110
lookup コマンド
アクセス
(a)
(b)
(c)
(d)

フロントページの続き

(72)発明者 岩田 真一
東京都八王子市大和田町３丁目１４番地１６号

Ｆターム(参考) 5B085 BA06
5K030 GA14 HA08 HD09 KA05 KA15 LD19 MD10